LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-643032

# Crystal Williams NNSA Essay

C. Williams

August 28, 2013

## Disclaimer



This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

# Summer Internship at Lawrence Livermore National Laboratory

By: Crystal Ronnette Williams – Software Engineering M.S. Student
Florida Agricultural & Mechanical University

Lawrence Livermore National Laboratory (LLNL), established in 1952 by the University of California, is known as a premier research and development institution for science and technology applied to national security. This lab is responsible for ensuring the safety, security and reliability of the nation's nuclear weapons through the application of advanced Science, Technology, Engineering and Mathematics (STEM). Along with this LLNL also supports various researches that develop new science and technologies to meet future national needs. With that being said I would like to thoroughly explain my amazing summer here at this prestigious lab.

**Project** Location Based Services (LBS) is a popular asset and necessity embedded in mobile devices today. Used to locate venues near you, access Global Positioning Services (GPS) and on most mobile devices allow your friends to know your exact whereabouts. This all seems convenient but causes privacy issues that are attracting major Computer Scientists across the country. This particular issue leads to, private proximity testing, which allows friends to be notified when they are in proximity of each other, but otherwise reveal no information about their locations to anyone. In this study we implemented several privacy protocols, in android environments, which provide privacy for location based services. With these implementations we also did performance analysis for each individual protocol.

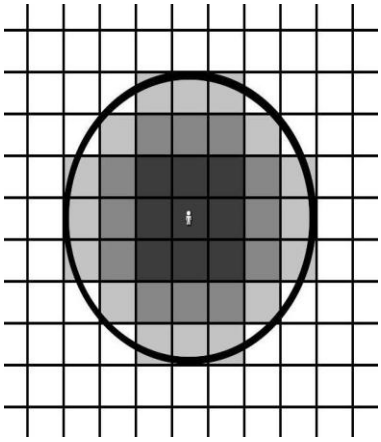

Figure 1 – Location is grid based; this defines the proximity of each peer

Prior to coming to the lab I was selected by a professor from the University of California, Dr. Levent Ertaul, to work on a team dealing with these protocols in the Android environment. My particular protocol, based on homomorphic ElGamal cryptosytem, was Active Secure Protocol. Designed to provide all parties with security when gathering knowledge of their associate's location. Allowing users to communicate directly without utilizing actual locations and notifying the user if their friend is/is not in the vicinity guarantees privacy because of the discrete log problem.

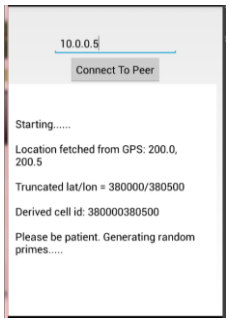


Figure 2 – Android Emulator searching for peer

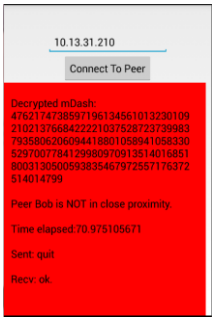


Figure 3 – Android Emulator after search is complete

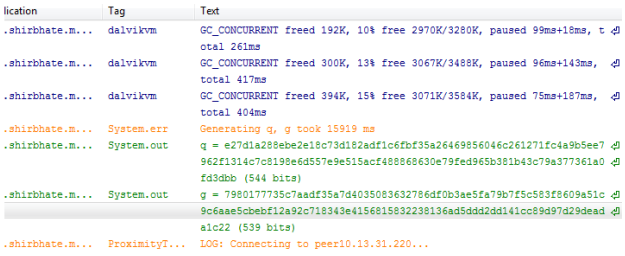


Figure 4 – Android Emulator debug showing length of variables and generator

I also performed analysis based testing for a 1:1 scenario by using an Android Emulator within Eclipse. As you can conclude from the results below, my implementation was not suitable for the android environment however, the security without a doubt guarantees privacy of the user's location.

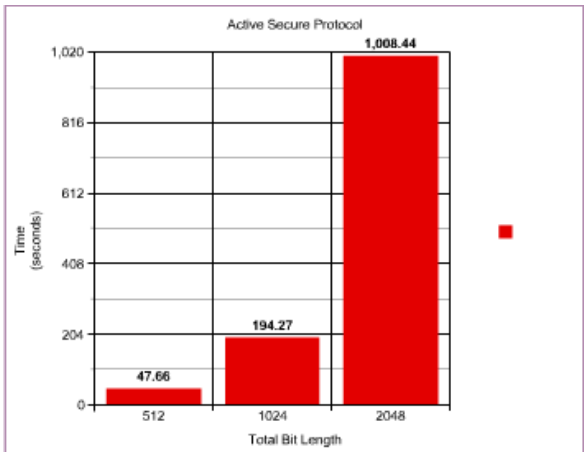


Figure 5 – Active Secure Protocol Performance analysis 1:1

I enjoyed this project so much that I hope to continue working on it once I return to my institution to find better techniques that will improve speed for the calculations, which will lead to a much better implementation. Along with that I will test the protocol for multiple users and install this on an actual device and test the performance that way as well.

With this project I was more exposed to cryptography and became knowledgeable of the discrete log problem. I also realized the difficulties that come along when taking cryptography and implementing the calculations. So overall this project was extremely challenging but I learned a heap of new programming skills that I can utilize in my near future as I continue my education.

**Cyber-Defenders** This is my second summer at the lab and I was fortunate enough to be apart of the Cyber-Defenders program here at the Lab. Within this program we are required to take and complete two courses, attend all seminars and compete in the "Capture the Flag" competition.

Network security was one of the required courses and it taught me a lot about ethical hacking and techniques on how to pass the certification exam if I ever intended to take it. Wireless Security was my second course and the curriculum was geared towards encryption protocols for wireless connections. Within the seminars I found the legal aspect of cyber-security the most interesting because there are so many malicious things done on-line not only to individuals but to major companies as well, which presents the need for legal action. The most interesting learning experience was definitely the "Capture the Flag" competition. Within this competition we were divided into six teams of five and given access to the same gaming system provided to our lab as well as Sandia National Laboratories in California and New Mexico. The jeopardy-like game was designed to test your learning skills and ability to solve technical issues on the spot. I learned so many new tools within this challenge such as wireshark, virustool.com and IDA pro. Not only did I learn about them but I simultaneously learned how to also use them which was amazing and showed me the potential within myself.

**MSI Seminars** Minority Serving Institutions is a program I was under here at the lab as well. Within this program there was a mandatory seminar every Tuesday during lunch and they all contributed in different ways to advancing ourselves mentally and with our education. From taking our skills and helping us to benefit others to building ourselves a stronger resume and presence. Every seminar was intriguing and helped me to strategically decide on pursuing a Ph.D., interviewing skills, self-motivating techniques and ways to better my life on a daily basis.

**LLNL Website** I was among one of the few students to be chosen as a featured student on the LLNL computation website. My summer internship project and experience will be on the lab's website along with a photo and information about my institution.

**ULearn** The lab offers a site to assist with learning new material. While awaiting my mentor's arrival I learned J-query and Java script while here at the lab as well. This is indeed a very powerful and beneficial programming language that I look forward to using in the future.

I had an amazing summer here at Lawrence Livermore National Laboratory and would encourage other students to come here to get a challenging internship that is guaranteed to help you educationally and with deciding career paths. I am grateful for this opportunity because it has helped me tremendously in so many aspects and gave me the exposure that I needed not only to a different environment but how to work and develop with real life scenarios.

## Disclaimer